УДК 621.396.1

А. С. Карамышев
Научный руководитель: ст. преп. Д. В. Ремизов
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ M2M

Аннотация. В данной статье исследуются возможные проблемы информационной безопасности в сетях M2M, требования, предъявляемые к данным сетям, а также методы обеспечения информационной безопасности. Внимание уделяется реализации сетей M2M на существующих сетях беспроводной связи и проблемам, возникающим при данной реализации.

Ключевые слова: информация; безопасность; сети M2M; аутентификация; конфиденциальность; целостность.

С развитием стандартов беспроводных сетей связи широкое распространение получили устройства, реализующие функции сбора, обработки и передачи информации как без участия, так и минимальным участием человека. Технологии взаимодействия таких устройств называют M2M (Machine-to-Machine, машинно-машинное взаимодействие), а сети, объединяющие данные устройства и обеспечивающие к ним доступ, — сетями M2M. Концепция устройств M2M подразумевает низкую стоимость, мобильность, низкое энергопотребление, а также передачу данных в локальных и глобальных беспроводных сетях. Помимо этого, необходима возможность удаленного доступа для контроля и управления функциями устройств.

Поскольку сети M2M зачастую реализуются на существующих сетях беспроводной связи, устройства подвержены угрозам безопасности со стороны сетей связи. Также добавляется физическое воздействие на устройства, т. к. устройства используются по большей части без участия конечного пользователя. Данные особенности работы устройств M2M приводят к образованию угроз их безопасности, которые можно условно разделить на три группы:

А. Физические атаки: воздействие на M2M устройства с точки зрения аппаратного обеспечения.

Б. Логические атаки: воздействие на функционирование M2M устройств с помощью изменения/влияния на программное обеспечение.

В. Атаки на данные пользователя: перехват конфиденциальных данных, модификация данных [1].

На основе различных угроз безопасности в сетях M2M Европейским институтом по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, ETSI) был сформирован ряд требований к системам M2M, предъявляемых для обеспечения безопасности M2M устройств:

1. Система M2M должна поддерживать взаимную аутентификацию ядра M2M и устройства M2M или шлюза M2M, а также одностороннюю аутентификацию устройства M2M или шлюза M2M с помощью ядра M2M. Например, между поставщиком услуг и объектом, запрашивающим услугу, может запрашиваться взаимная аутентификация. Стороны могут выбрать степень аутентификации для обеспечения соответствующего уровня безопасности.

2. Система M2M должна поддерживать подтверждение целостности обменных данных.

3. Решение безопасности M2M должно предотвращать несанкционированное использование устройства/шлюза M2M.

4. Система M2M должна обеспечивать защиту конфиденциальности. Система M2M должна обеспечивать, чтобы данные приложений в системе M2M были доступны только для их предполагаемых получателей.

5. Множество действующих лиц участвуют в сквозной службе M2M. Система M2M должна позволять таким различным участникам предоставлять услугу в сотрудничестве, обеспечивая безопасность сквозного обслуживания, обеспечивая при этом конфиденциальность данных.

6. Система M2M должна поддерживать механизм проверки целостности M2M устройства/шлюза. Устройство/шлюз M2M может поддерживать или не поддерживать проверку целостности Если устройство/шлюз M2M поддерживает проверку целостности, и, если проверка M2M устройства/шлюза не выполняется, M2M устройство/шлюз не разрешается выполнять аутентификацию M2M Device/Gateway.

7. M2M устройства/шлюзы, для которых требуется проверка целостности, должны предоставить доверенную среду для этой цели.

8. В тех случаях, когда это разрешено политикой безопасности, система M2M должна иметь возможность удаленно предоставлять следующие функции на уровне приложения:

- безопасные обновления программного обеспечения безопасности приложений и прошивки устройства M2M/шлюза;
- безопасное обновление контекста безопасности приложения (ключей и алгоритмов безопасности) устройства M2M/шлюза.

Эта функциональность должна обеспечиваться защищенной от несанкционированного доступа средой (которая может быть независимым элементом безопасности) в устройствах/шлюзах M2M, поддерживающих эту функциональность.

9. Решение безопасности M2M должно обеспечивать защиту ядра M2M от таких атак, как отказ в обслуживании и неправильное использование, клонирование или кража учетных данных.

10. Наличие приложений, работающих на ресурсах, принадлежащих другой системе M2M, должно соответствовать требованиям безопасности собственной и других систем M2M. Конфиденциальность использования ресурсов должна поддерживаться в случае приложений, работающих на ресурсах, принадлежащих разным системам M2M [2].

В соответствии с требованиями выделяют следующие методы обеспечения безопасности сетей M2M:

- различные виды шифрования и хеширования для обеспечения защиты целостности и приватности;
- несколько вариантов аутентификации для контроля доступа;
- фильтрация трафика, генерируемого сетями M2M;
- использование сим-карт для обеспечения приватности в сетях мобильной связи [3].

Консорциум 3GPP (3rd Generation Partnership Project), а также организация ETSI выдвинули свои варианты решений по повышению информационной безопасности в сетях M2M. Их решения основаны на описанных выше методах и включают обоснования введения независимого оборудования для построения сетей, такого как M2M домены, серверы AAA (Authentication, Authorization, Accounting) и шлюзы для обеспечения взаимодействия с существующими сетями связи.

Список литературы

1. *Barki A.*, *Bouabdallah A.*, *Gharout S.*, *Traore J.* M2M Security: Challenges and Solutions // IEEE Communications Surveys & Tutorials. 6 January 2016. Vol. 18, Is. 2. P. 1241–1254.

2. Machine-to-Machine communications (M2M) // M2M service requirements ETSI TS102689 V2.1.1 (2013–07). 35 p.

3. *Тихвинский В. О.*, *Коваль В. А.*, *Бочечка Г. С.*, *Бабин А. И.* Сети IoT/M2M: технологии, архитектура и приложения. М. : Изд. дом «Медиа Паблишер», 2017. 320 с.